WEB OF SCIENTIST: INTERNATIONAL SCIENTIFIC RESEARCH JOURNAL
ISSN: 2776-0979, Volume 4, Issue 12, December, 2023

METHODOLOGY FOR ASSESSING INFORMATION SECURITY RISKS OF EXTERNAL PROGRAM INTERFACES OF SDN CONTROLLERS

D. T. Khakimbekov
Master student of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract
A methodology for assessing and managing the risks of software - defined networks is proposed. The proposed methodology is capable of assessing the risk associated with service requests received through the northbound interface of the SDN controller.

Keywords: interface, SDN, topology, matrix service, controller, switch.

Introduction

The concept behind software-defined networking (SDN) is to separate the control plane from the data plane. The control plane is represented by a logically centralized controller, and the data plane consists of SDN switches, which, unlike classic switches, only forward packets without making decisions about their direction. This approach makes it possible to implement global routing policies without the need to configure each device individually [1].

The interface that allows the controller to interact with external applications is called the northern interface in SDN terminology. It provides ample opportunities for automation and flexible network management. For example, using the northern interface, services can inform the controller about expected changes in the volume of incoming traffic. However, such changes may not occur even if SDN allocates resources to clients and traffic flows. Such unnecessary rearrangements of the virtual network topology negatively affect its performance - reserving unclaimed resources worsens service parameters (such as latency, bandwidth) for other network nodes. Therefore, it is important to develop a critical approach to evaluate the information provided by services to the SDN controller [2,3].

Method

Existing risk assessment methodologies are not applicable to software-defined networks because they focus only on traditional networks and do not take into account the dynamic nature of SDN. Based on this, it is advisable to develop an effective mechanism for assessing the security of SDNs, taking into account their

distinctive features. To make decisions regarding requests received by the controller from external services, this article proposes an approach to risk assessment and management. 89 II I III IV Level of trust in the service Degree of topology change In the context of information coming from applications through the external interface, two factors can be identified that determine the risk of an incoming request: the negative impact on the network and the likelihood of the threat being realized [4,5]. Negative impact is a factor associated with SDN network rebuilds and its final topology. When a service requests new bandwidth parameters, the virtual network topology changes. Processing such a request may result in the allocation of significant resources and the need to rebuild the network. As a result, the quality of service for other customers may be degraded. Therefore, the impact factor is related to the global status of the entire SDN network, and its quantitative assessment is related to the network optimization criteria, i.e. using controller resources, bandwidth and delays.

Results and discussion

Network optimization tools are capable of determining the optimal virtual topology for data flow under given conditions. If the service reports that the volume of traffic between a certain pair of nodes will change in a certain way, the optimization tool will suggest an optimal virtual topology for the new conditions. The resulting value of the objective function characterizes the final state of the network (under given conditions). This value allows us to determine a quantitative approach to assessing the negative impact factor. However, in reality, the traffic between a given pair of nodes may not change, despite a preliminary request from the service and a recalculation of the network topology.

If we assume that the service can correctly predict changes in traffic volumes, or, on the contrary, do this completely incorrectly, it is possible to consider four different scenarios, schematically presented in Fig. 1.

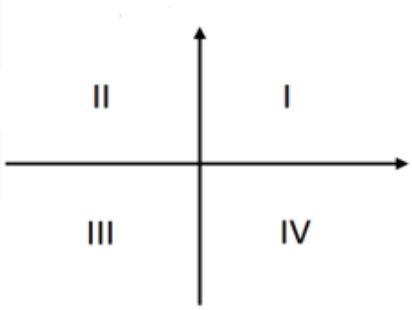

Fig. 1. Scenarios of correct and incorrect traffic volume forecasts

I. The virtual network topology has changed and the required bandwidth has changed according to the request. The volume of incoming traffic has changed in accordance with the forecast, so confidence in the service should increase.
II. The virtual network topology has not changed, but the traffic flow has changed in accordance with the service forecast. In this case, the network topology is not 90 optimal (conditions have changed), but trust in the service should increase because the volume of traffic has changed as expected.
III. The virtual network topology has not changed even though the external application requested the change. This occurs when the existing topology is still optimal for the requested changes. In this scenario, trust in the service will be reduced if subsequent changes in traffic volumes do not match the forecast.
IV. The virtual network topology has changed, but the volume of incoming traffic has not changed, despite the request. The service's actions led to an unreasonable restructuring, so trust in it should decrease.
The considered scenarios assume that the service predicted traffic changes correctly or completely incorrectly. However, intermediate states are also possible: the traffic flow may change, but to a lesser extent than predicted by the service. Therefore, it is also necessary to consider optimal virtual topologies for minor changes in data flow in order to provide optimal conditions according to the request of the external application. Accurate estimation requires determining intermediate states for the received request. To do this, it is necessary to define a matrix I containing network states for various scenarios:

$$I = \begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \beta_1 & \beta_2 & \cdots & \beta_m \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1 & \omega_2 & \cdots & \omega_m \end{bmatrix} \quad (1)$$

where α, β, ... ω mean different virtual topologies, and m is the number of intermediate states. Thus, each row represents a strictly defined virtual topology (optimized for a specific volume of incoming traffic), and each column represents the volume of predicted incoming traffic. As a result, each element in the matrix contains a numeric value that characterizes the bandwidth requirements and network topology.
The likelihood of a threat being realized is related to the service that sends the request, and therefore depends on the level of trust in it. As a measure of quantitative assessment of trust in a service, it is proposed to use a reputation system, which establishes the degree of trust of each registered service.

WEB OF SCIENTIST: INTERNATIONAL SCIENTIFIC RESEARCH JOURNAL
ISSN: 2776-0979, Volume 4, Issue 12, December, 2023

The reputation of a service is formed as requests are received from it, and should allow applications to be classified not only as trusted or untrusted , but also as partially trusted. Therefore, the reputation of each object can be denoted by a number in the range [0,1]. A value of 1 indicates a completely reliable service, and a value of 0 indicates a completely unreliable service. The new object will be given an initial value (eg 0.5), but it will change dynamically based on the object's behavior. The reputation system should accept as input requests that are relevant to 91 SDN networks: providing reliable and useful messages will increase the level of reputation, if information about traffic changes is incorrect, the reputation will decrease.

Matrix I (1) contains network states for scenarios with different bandwidth requirements between the node pair under consideration. Therefore, it is also necessary to define a matrix L containing the confidence level for each request containing a forecast about changes in traffic volumes:

$$L = \begin{bmatrix} l_1 & l_2 & \cdots & l_m \\ l_1 & l_2 & \cdots & l_m \\ \vdots & \vdots & \ddots & \vdots \\ l_1 & l_2 & \cdots & l_m \end{bmatrix} \qquad 2)$$

where m is an indicator of the degree of change in traffic volumes between a given pair of nodes. This matrix is specific to the service that sends requests through the controller's northbound interface, and the values in it are directly related to the level of trust in them, as well as to the probability distribution that characterizes the service's ability to predict the volume of incoming traffic.

The level of risk can be defined as the product of two factors: negative impact and probability of implementation. The proposed methodology assumes that the negative impact is due to the change in network state that occurs as a result of the requested bandwidth and the probability that is associated with the level of trust in the requester.

The row numbers in matrices I and L are identical and indicate the number of virtual topologies under consideration. Thus, taking into account the same sizes of matrices I and L, we can define the risk assessment matrix R as the product of matrix I, representing the negative impact factor, and matrix L, representing the probability factor of the threat:

$$R = I \times L = \begin{bmatrix} \alpha_1 \times l_1 & \alpha_2 \times l_2 & \cdots & \alpha_m \times l_m \\ \beta_1 \times l_1 & \beta_2 \times l_2 & \cdots & \beta_m \times l_m \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1 \times l_1 & \omega_2 \times l_2 & \cdots & \omega_m \times l_m \end{bmatrix} = \begin{bmatrix} r_{1,\alpha} & r_{2,\alpha} & \cdots & r_{m,\alpha} \\ r_{1,\beta} & r_{2,\beta} & \cdots & r_{m,\beta} \\ \vdots & \vdots & \ddots & \vdots \\ r_{1,\omega} & r_{2,\omega} & \cdots & r_{m,\omega} \end{bmatrix} \qquad 3)$$

The matrix R defines the risk value for each considered traffic change in all predicted virtual topologies. Therefore, it is necessary to summarize the risks for each topology:

$$R_j = \sum_{i=1}^{m} R_{i,j} \quad j = \alpha, \beta, \dots, \omega \qquad 4)$$

Conclusion

The proposed approach allows us to find a scenario with the lowest level of risk. Such calculations can be performed for the original topology (unchanged network) and for predicted structures, including intermediate ones. The results will show which network structure is the most secure, that is, 92 where the level of risk is minimal. Using the proposed methodology, the SDN network is able to make the best decision regarding the requests received from the northbound interface of the controller.

References

1. Javier Guillermo. How 5G Relates to SDN and NFV Technologies – Part I: Introduction and History. DELL Technologies, 2019. https://infocus.delltechnologies.com/javier_guillermo/how-5g-relates-to-sdn-andnfv-technologies-part-i-introduction-and-history
2. Pradhan, A., Mathew, R. Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN). Procedia Computer Science, Vol . 171, 2020. https://doi.org/10.1016/j.procs.2020.04.280
3. Shahryari , S., Hosseini-Seno, S.-A., Tashtarian , F. An SDN based framework for maximizing throughput and balanced load distribution in a Cloudlet network. Future Generation Computer Systems, Vol. 110, September 2020. https://doi.org/10.1016/j.future.2020.04.009
4. Semenovykh A.A., Laponina O.R. Comparative analysis of SDN controllers. INJOIT. 2018. T. 6. No. 7. P. 50–56 (Russian)
5. Introduction to Software Defined Networks (SDN). URL: https://www.researchgate.net/publication/311479628_Introduction_to_Software_Defined_Networks_SDN. DOI: 10.5120/ijais2016451623 (date requests : 03/11/2020)